

REMARKS

Claims 1-20 remain pending in the application. All claims stand rejected.

Claim Rejections – 35 USC § 103

The following is a quotation from the MPEP setting forth the three basic criteria that must be met to establish a *prima facie* case of obviousness.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. MPEP, §2142, citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Claims 1-20 stand rejected under 35 USC §103 over CyberCop Scanner by Network Associates as described in the Info World article entitled “Test Center Comparison” (hereinafter, “CyberCop”) in view of Info World article entitled “The Ins and Outs of a Network Security Audit” (hereinafter, “Security Audit”). Applicants respectfully disagree and traverse the rejection since, among other reasons, Security Audit and CyberCop do not teach every element of the claims and are not reasonably combined (i.e., no reasonable expectation of success) to render, teach or suggest Applicants' claims.

In particular, claim 1 is a security system for a computer apparatus, wherein said computer apparatus includes a processor and system memory, and includes:

- (A) at least one security module which under direction from the processor accesses and analyzes selected portions of the computer apparatus to identify vulnerabilities;

- (B) at least one utility module which under the direction from the processor, performs various utility functions with regards to the computer apparatus in response to the identified vulnerabilities; and
- (C) a security system memory which contains security information for performing the analysis of the computer apparatus.

CyberCop discloses an Internet Scanner. The Examiner refers to page 2 of CyberCop, 4th paragraph from the last, as if that section teaches element A of claim 1. We disagree. There is no teaching in this section of CyberCop of "at least one security module which under direction from the processor accesses and analyzes selected portions of the computer apparatus to identify vulnerabilities." Where, for example, does CyberCop disclose analyzing "selected portions" of a computer apparatus? CyberCop does not in fact disclose this feature, among others, of claim 1.

The Examiner further relies on CyberCop page 3, second from last paragraph, in asserting that CyberCop teaches element C of claim 1. We again disagree. Memory is not even mentioned in this paragraph (or elsewhere in the context of claim 1).

The Examiner then states that the "article implies" the disclosure of suggesting fixes. First of all, this is not text of claim 1. Secondly, we contend that such assertions are not consistent with 35 U.S.C. §103 (or 102). One cannot read into text and make an allegation that it implies something. We therefore must ask for evidence consistent with the Examiner's broad assertions that one skilled in the art would somehow render claim 1 (and other claims) by "implications" of CyberCop. We disagree; and we are permitted to ask for this evidence pursuant to MPEP §2144.

Moreover, the "manual activity" that is alleged within CyberCop is not consistent with the elements of claim 1 (or other claims for that matter). CyberCop is being read within considerable hindsight in the allegations set forth in the pending office action.

On page 2 of the current office action, the Examiner goes to great lengths to describe steps that are not equivalent to elements of claim 1. We are, therefore, quite confused about the intent of these statements. The allegations of "one skilled in the art" must therefore be more firmly supported with evidence of actual motivation as to what exactly one skilled in the art knows, as of the date of the invention of the claims, because the teachings of CyberCop and Security Audit (see below) are clearly insufficient to teach the elements of the claims (claim 1 and the other rejected claims).

Security Audit describes the auditing of a network and, in particular, the following: (a) security policy issues, (b) examination of a test network, and (c) the interpretation of reports. "Our focus in this article is mainly on the process and the tools that make up a successful audit." Security Audit, page 1, 4th paragraph. These elements a-c do not, in any way, teach or suggest elements A-C of claim 1. Note specifically that claim 1 requires a security module, utility module and security system memory, among other features, that are entirely absent within Security Audit.

On page 2, 4th paragraph, Security Audit discusses "tools you should use to carry out an effective security audit." The specific tools tested were "manager/agent" and "network scanner." See Security Audit, page 3, 2nd paragraph. The Examiner seems to lean on page 4, 1st paragraph, as if Security Audit teaches a configuration and vulnerability baseline. First of all, these are not textual elements described in claim 1. Secondly, Security Audit does not even disclose what the Examiner alleges: specifically, the section that the Examiner relies on refers to "reams of text" and "graphs" about exploitable holes in the database and that these items should be stored in a "secure place" for comparison to the next audit. A "secure place" is not a security system memory as claimed in claim 1. The way it is written, one could easily imply that the secure place is a locked office.

In summary, the Examiner has not shown that CyberCop and/or Security Audit teaches elements A-C of claim 1. This is absolutely required under 35 U.S.C. §103. Moreover, the Examiner has used hindsight in the allegations set forth in the rejections of claim 1. Further, we must insist on evidence supporting the Examiner's allegations of what one skilled in the art could reasonably do with CyberCop or Security Audit because, at least, these two papers do not teach the elements of the claims. How can there be a reasonable chance of success if even the elements are not taught or described? Even the Examiner's recitation of elements on page 2 of the pending action do not mirror elements of the claims.

Reconsideration of claim 1 is requested.

Claims 2-10 depend from claim 1 and benefit from like arguments; but these claims also have additional features which patentably distinguish over the art. In rejecting these claims, the Examiner again relies on hindsight and allegations of "one skilled in the art" – so we again must ask for evidence pursuant to MPEP §2144 to support these allegations. A thorough reading of both CyberCop and Security Audit clearly illustrates that the articles do not teach the elements of these claims in the context of independent claim 1.

Reconsideration of claims 2-10 is also requested.

Claim 11, the other independent claim of this pending application, requires the following step elements in a method of providing a security assessment for a computer system which includes a system memory:

providing a security subsystem in the computer system such that functionality of the security subsystem is directed through a processor for the computer system, wherein the security performs steps comprising:
identifying a configuration of the system;
accessing the system memory and performing at least one procedure to provide a security assessment for at least one aspect of the computer system;

as a result of any vulnerabilities discovered in the assessment, identifying corrective measures to be taken with regards to the computer system;

reporting the discovered vulnerability and the identified corrective measures; and

upon receiving an appropriate command, initiating the corrective measures.

First of all, all the foregoing arguments in connection with claim 1 also apply here. For example, where is a "memory" (in the context of claim 12) taught in CyberCop or Security Audit?

Secondly, on page 2 of the pending action, the Examiner has made statements of steps that are quite inconsistent with the steps of claim 12. We again therefore must insist on evidence (pursuant to MPEP §2144) supporting the Examiner's allegations because, among other reasons, we contend that these allegations rely on impermissible hindsight.

For example, the following two step elements of claim 12 are, clearly, not taught or suggested by CyberCop or Security Audit: "identifying corrective measures..." and "initiating the corrective measures." Where are these elements taught in either CyberCop or Security Audit? Neither the articles themselves or the Examiner's comments provide any guidance to support the 35 U.S.C. §103 rejection.

Claims 12-20 depend from claim 11 and benefit from like arguments; but these claims also have additional features which patentably distinguish over the art. As above, in rejecting these claims the Examiner again relies on hindsight and allegations of "one skilled in the art" – so we again must ask for evidence pursuant to MPEP §2144 to support these allegations. A thorough reading of both CyberCop and Security Audit clearly illustrates that the articles do not teach the elements of these claims in the context of independent claim 11.

Reconsideration of claims 11-20 is requested.

In view of the above Remarks, Applicants have addressed all issues raised in the Office Action dated May 18, 2004, and respectfully solicit a Notice of Allowance for claims 1-20. Should any issues remain, the Examiner is encouraged to telephone the undersigned attorney.

A Petition for three month's extension of time to reply is submitted herewith, extending the period for reply up to and including November 18, 2004. Authorization to charge the necessary fee of \$490 for a small entity to Deposit Account 12-0600 is granted within the attached Petition for three month's extension of time. It is believed that no further fees are due; however, if any additional fee is required in connection with this Amendment and Response, the Commissioner is further authorized to charge such fee to Deposit Account 12-0600.

Respectfully submitted,

Date: 18 Nov 2004

By:

Curtis A. Vock
Curtis A. Vock, Reg. No. 38,356
LATHROP & GAGE L.C.
4845 Pearl East Circle, Suite 300
Boulder, CO 80301
Telephone: (720) 931-3011
Facsimile: (720) 931-3001